



PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES – PDTIC

2025/2027

(versão atualizada – junho/2025)

**PREFEITURA DO MUNICÍPIO DE BRAGANÇA PAULISTA
SECRETARIA MUNICIPAL DE GOVERNO, DESENVOLVIMENTO ECONÔMICO E
INOVAÇÃO - DIVISÃO DE INOVAÇÃO E TECNOLOGIA**

Projeto do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), realizado pela Secretaria Municipal de Governo, Desenvolvimento Econômico e Inovação, como parte da adequação das normas vigentes com relação ao instrumento de diagnóstico, planejamento e gestão de recursos e processo de Tecnologia da Informação e Comunicação, atendendo as necessidades tecnológicas do Município de Bragança Paulista.

COLABORADORES

André Elesbão

SECRETÁRIA DE GOVERNO, DESENVOLVIMENTO ECONÔMICO E INOVAÇÃO

Everton Ferrira

CHEFE DA DIVISÃO DE INOVAÇÃO E TECNOLOGIA

SUMÁRIO

1. INTRODUÇÃO

2. OBJETIVO

PETI – PLANEJAMENTO ESTRATÉGICO DA TECNOLOGIA DA INFORMAÇÃO

3. REFERENCIAIS ESTRATÉGICAS DA DIVISÃO DE INOVAÇÃO E TECNOLOGIA

- 3.1 MISSÃO
- 3.2 VISÃO
- 3.3 VALORES
- 3.4 NEGÓCIO
- 3.5 EQUIPE PARTICIPANTE
- 3.6 PARTES INTERESSADAS
- 3.7 METODOLOGIA APLICADA
- 3.8 ORGANOGRAMA ESTRUTURAL DA GESTÃO ATUAL DA TECNOLOGIA DE INFORMAÇÃO
- 3.9 DA INFORMAÇÃO E COMPETÊNCIAS
 - 3.9.1 Secretária de Governo, Desenvolvimento Econômico e Inovação
 - 3.9.2 Chefe da Divisão de Inovação e Tecnologia
 - 3.9.3 Suporte Técnico e Redes de Computadores
 - 3.9.4 Equipe Administrativa
 - 3.9.5 Equipe de Sistemas
- 3.10 OBJETIVOS

2. DIAGNÓSTICO DE TECNOLOGIA DA INFORMAÇÃO

- 4.1 INTRODUÇÃO
- 4.2 VISÃO GERAL
- 4.3 INFRAESTRUTURA
 - 4.3.1 ESTAÇÕES DE TRABALHO E SERVIDORES
 - 4.3.2 ESTRUTURAS DE REDE DA PREFEITURA DE BRAGANÇA PAULISTA
 - 4.3.3 SISTEMAS PRÓPRIOS E TERCEIRIZADOS UTILIZADOS PELA PREFEITURA DO MUNICÍPIO DE BRAGANÇA PAULISTA
 - 4.3.4 SEGURANÇA
 - 4.3.5 BACKUP

- 4.3.6 PESSOAS E PROCESSOS

3. INFRAESTRUTURA FÍSICA E LÓGICA DA REDE DE COMPUTADORES

4. REDE FÍSICA

5. SEGURANÇA

6. FIREWALL DE PERÍMETRO

7. TRABALHO REMOTO

8. CONTROLE DE ACESSO À REDE

9. INVENTÁRIO

10. MONITORAMENTO DA REDE DE DADOS

11. POLÍTICA DE SEGURANÇA

12. PLANO DE CONTINUIDADE DE NEGÓCIO

13. CONSIDERAÇÕES FINAIS

ANEXO – ORÇAMENTO – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E
COMUNICAÇÃO – PJ – EXERCÍCIOS 2025, 2026 E 2027

1. INTRODUÇÃO

O Plano Diretor de Tecnologia da Informação e Comunicações (PDTIC) é um instrumento de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação que visa atender às necessidades tecnológicas e de informação da Prefeitura de Bragança Paulista. Este PDTIC, que será aplicado para os anos de 2025, 2026 e 2027, está alinhado às diretrizes estratégicas da Prefeitura de Bragança Paulista e prevê a ocorrência de revisões periódicas, ensejadas pelo surgimento de novos cenários, diretrizes e prioridades.

A missão da Prefeitura Municipal de Bragança Paulista é prestar serviços de forma eficaz e transparente aos cidadãos bragantinos. Para isso, traçamos metas a fim de dispor aos funcionários ferramentas que melhorem o ambiente de trabalho e, por consequência, que permitam a prestação do melhor atendimento aos munícipes de Bragança Paulista.

Além disso, temos como meta realizar a gestão de contratos voltados à tecnologia da informação com transparência, promovendo sempre as melhores ferramentas e recursos tecnológicos ao município.

Contamos com equipes engajadas proporcionando um trabalho eficaz na prestação de nossos serviços, bem como na busca das melhores tecnologias do mercado para atender as demandas internas e externas.

As constantes transformações do mundo globalizado têm feito com que as organizações, também da gestão pública, se preocupem cada vez mais em identificar a melhor forma de empregar seus recursos, buscando a melhoria na qualidade dos serviços prestados ao cidadão. Isso significa melhorias no ambiente da gestão pública pelo aumento da eficácia organizacional: agilidade nos processos, na estrutura, na comunicação e na eliminação da burocracia.

O uso estratégico da tecnologia da informação e a administração dos recursos de informática podem e devem melhorar o atendimento da população e o desenvolvimento sustentável deste município.

Nesse contexto, a Tecnologia da Informação (TI), que durante muito tempo foi considerada apenas um item de suporte aos processos internos, uma fonte de despesas, sem influência direta nos objetivos e metas da gestão pública, deve ser repensada como um fator crítico para a prestação de serviços públicos, resultando em crescimento da atuação do poder público, exercendo assim um forte domínio sobre os interesses da população.

Este Plano Diretor de Tecnologia da Informação foi desenvolvido a partir de levantamento e análise da situação organizacional e tecnológica, realizado em 2022 e atualizado ao longo do ciclo 2022–2024, servindo como base para o presente ciclo 2025–2027. O levantamento da situação tecnológica contemplou:

- Análise do Parque Computacional;
- Análise da arquitetura de sistemas;
- Análise da infraestrutura de redes;
- Identificação dos recursos de *hardware*, *software* básico e aplicativos;
- Estudo de documentos da área de informática.

Nos últimos anos, a área de informática da Prefeitura Municipal de Bragança Paulista vem passando por vários processos de reorganização, realinhamento tecnológico e de infraestrutura física do parque computacional, para gerar condições para cumprir sua missão e seu plano estratégico.

O mercado tecnológico indica como tendências aplicáveis à atuação dos órgãos públicos, no decorrer dos anos, redes com alta velocidade, interoperabilidade de aplicações, maior produtividade, sistemas de gerência de bancos de dados de grande capacidade de armazenamento, segurança da informação, alto nível de conectividade e interação com novas linhas de atuação através de canais virtuais e governo eletrônico, além de computação em nuvem, mobilidade, análise de dados e inteligência artificial aplicada aos serviços públicos.

Para que as recomendações propostas pelo PDTIC sejam viáveis, é de suma importância a disponibilização de um orçamento anual para investimento em Tecnologia da Informação, compatível com as necessidades, equiparando-se assim ao mesmo patamar da evolução tecnológica dos demais órgãos municipais, estaduais e federais.

A partir desta atualização do PDTIC, passamos a contemplar o orçamento destinado a todas as secretarias municipais, especificamente com relação aos valores previstos e orçados para os exercícios de 2025, 2026 e 2027 com serviços de tecnologia da informação e comunicação – pessoa jurídica. Este orçamento garante que as ações estipuladas neste PDTIC sejam realizadas. O orçamento total previsto para essa rubrica é de **R\$ 12.812.634,45 (doze milhões, oitocentos e doze mil, seiscentos e trinta e quatro reais e quarenta e cinco centavos)**, sendo que deste valor a quantia de **R\$ 2493493,8** (dois milhões, quatrocentos e noventa e três mil, quatrocentos e noventa e três reais e oitenta centavos), é proveniente de recursos vinculados das Secretarias de Educação, Saúde e Ação e Desenvolvimento Social.

As planilhas detalhadas do orçamento previsto para os exercícios de 2025, 2026 e 2027 seguem acostadas ao final deste plano.

O PDTIC deverá ser avaliado a cada triênio e ajustado para melhor atendimento dos serviços prestados pela área de TI. O presente documento foi atualizado em janeiro de 2025 para orientar o novo ciclo de planejamento 2025–2027.

Os aspectos táticos e operacionais decorrentes do PDTIC serão definidos em etapa posterior, em conjunto com representantes das secretarias da Prefeitura do Município de Bragança Paulista.

Além de alcançar as metas estabelecidas neste PDTIC, é válido ressaltar a importância em estreitar o relacionamento com as diversas secretarias da Prefeitura desta municipalidade.

2. OBJETIVO

Apresentar propostas que auxiliem na instauração de um processo de melhoria contínua nos itens de *software*, *hardware*, administração da rede, infraestrutura, banco de dados e segurança da informação, apontando soluções para os problemas identificados que estejam limitando o alcance das metas da Prefeitura de Bragança Paulista, por meio da Divisão de Inovação e Tecnologia.

Este PDTIC será o documento norteador para elaboração do planejamento e execução de todas as ações da tecnologia da informação da Prefeitura Municipal de Bragança Paulista no triênio 2025–2027.

PETI – PLANEJAMENTO ESTRATÉGICO DA TECNOLOGIA DA INFORMAÇÃO

3. REFERENCIAIS ESTRATÉGICAS DA DIVISÃO DE INOVAÇÃO E TECNOLOGIA

3.1 MISSÃO

A missão da Divisão de Inovação e Tecnologia (DIT) é garantir a manutenção, implementação e a melhoria contínua da infraestrutura tecnológica da cidade, aprimorando a eficácia da administração pública e a qualidade dos serviços prestados à população, seguindo as diretrizes de governança e adotando tecnologias emergentes para aprimorar os serviços.

3.2 VISÃO

A visão da Divisão de Inovação e Tecnologia é ser referência na implementação de soluções tecnológicas inovadoras que impulsionem a transformação digital da cidade, tornando-a mais conectada, sustentável e inteligente e, assim, proporcionando uma melhor qualidade de vida para a população.

3.3 VALORES

Os valores da Divisão de Inovação e Tecnologia incluem:

- Inovação e criatividade na busca por soluções tecnológicas eficazes e eficientes;

- Comprometimento com a excelência na prestação de serviços;
- Trabalho em equipe e colaboração com os diferentes setores da prefeitura;
- Ética e transparência nas atividades desenvolvidas;
- Responsabilidade socioambiental e sustentabilidade;
- Atualização constante e busca pelo conhecimento em tecnologia.

3.4 NEGÓCIO

O negócio da Divisão de Inovação e Tecnologia é prover soluções tecnológicas inovadoras para a administração pública da cidade, a fim de aumentar a eficiência e a eficácia dos serviços prestados, tornando a cidade mais conectada, sustentável e inteligente e, assim, proporcionando uma melhor qualidade de vida para a população.

3.5 EQUIPE PARTICIPANTE

NOME	CARGO	ÁREA
Edmir Chedid	Prefeito Municipal	Gabinete
Secretariado Municipal	Prefeitura Municipal	Todas as secretarias
André Elesbão	Secretária Municipal	Secretaria Municipal de Governo, Desenvolvimento Econômico e Inovação
Everton Ferreira	Chefia	Divisão de Inovação e Tecnologia
Lais Fernanda de Oliveira Felipe Santos Xavier Alexandre Soares Fabricio Cruz Moreira Lorenzo Alvarenga Mateus Ségur	Colaboradores da Divisão de Inovação e Tecnologia	Divisão de Inovação e Tecnologia (DIT)

3.6 PARTES INTERESSADAS

NOME	ÓRGÃO	CARGO
------	-------	-------

Gabinete do Prefeito	Prefeitura Municipal	Prefeito
Secretariado Municipal	Prefeitura Municipal	Todas as secretarias
Divisão de Inovação e Tecnologia	Prefeitura Municipal	Chefia e colaboradores

3.7 METODOLOGIA APLICADA

Para a elaboração deste PDTIC 2025–2027, a Prefeitura Municipal de Bragança Paulista norteou suas ações no modelo proposto pelo Guia de Elaboração de PDTIC do SISP, versão 2.1 – 2021, do então Ministério da Economia.

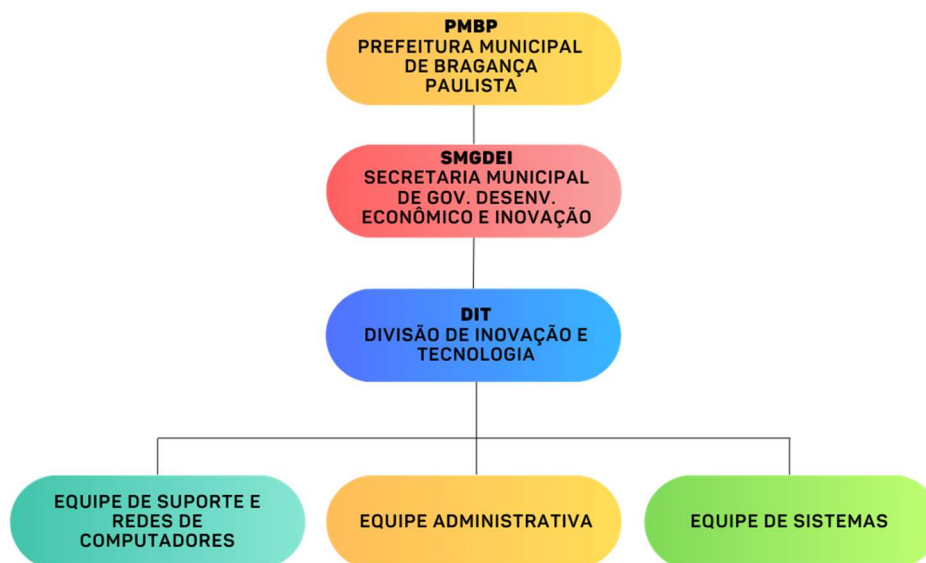
Para a criação deste plano, seguiram-se as seguintes etapas:

- Preparação;
- Diagnóstico;
- Planejamento.

A estratégia de elaboração do PDTIC foi seguir uma visão macro no primeiro ciclo, com melhor detalhamento na continuidade das ações, motivado pela amplitude e complexidade da área de TIC na Prefeitura.

3.8 ORGANOGRAMA ESTRUTURAL DA GESTÃO ATUAL DA TECNOLOGIA DE INFORMAÇÃO

ORGANIZAÇÃO ATUAL DIT



3.9 DA INFORMAÇÃO E COMPETÊNCIAS

3.9.1 Secretária de Governo, Desenvolvimento Econômico e Inovação

Competência: Assessorar o Chefe do Executivo em assuntos de sua unidade, planejar, organizar, coordenar e controlar a execução das atividades do setor, providenciando os meios para que as mesmas sejam realizadas; zelar pelo material e/ou equipamento pertencentes ao Setor; elaborar relatório periódico sobre as atividades de sua unidade; atender ao público em assuntos de competências de sua unidade; manter elevada a moral de seus subordinados e a colaboração entre os servidores municipais.

3.9.2 Chefe da Divisão de Inovação e Tecnologia

Competência: gerir a equipe de tecnologia da informação, garantindo que ela esteja apta a desenvolver, implementar e manter soluções tecnológicas que atendam às necessidades da administração pública e da população da cidade.

Dentre as principais responsabilidades do chefe da Divisão de Inovação e Tecnologia estão:

- Definir e implementar políticas e estratégias de tecnologia da informação para a administração pública da cidade;

- Gerir e monitorar o orçamento da divisão de informática, a fim de garantir que os recursos sejam utilizados de forma eficaz;
- Coordenar as atividades da equipe de TI, garantindo que ela esteja alinhada com os objetivos estratégicos da administração pública e entregue projetos no prazo e dentro do orçamento;
- Garantir que os sistemas de informação sejam seguros e estejam em conformidade com as leis e regulamentos aplicáveis;
- Identificar novas tecnologias e tendências para aprimorar a infraestrutura tecnológica da cidade;
- Estabelecer e manter parcerias com outras entidades governamentais e organizações do setor privado, visando colaborações em projetos e soluções de tecnologia da informação.

3.9.3 Suporte Técnico e Redes de Computadores

Competência: Prover a continuidade dos serviços tecnológicos, das quais destacamos:

Atendimento a usuários: responder a chamados de usuários com problemas técnicos, prestando suporte e solucionando as questões apresentadas, seja por telefone, e-mail, *ticket* de suporte ou presencialmente;

Diagnóstico de problemas: identificar a causa raiz dos problemas reportados pelos usuários e encontrar soluções adequadas, utilizando ferramentas e recursos disponíveis, incluindo a documentação técnica e a consulta a outros especialistas de níveis superiores;

Configuração e instalação/customização de software e hardware: configurar e instalar *softwares* e *hardwares*, como sistemas operacionais, aplicativos, impressoras, *scanners*, servidores, roteadores e *switches*;

Manutenção preventiva: realizar manutenção preventiva em equipamentos de TI, como atualização de sistemas operacionais e aplicativos, limpeza física, *backup* de dados e monitoramento de segurança;

Gerenciamento de rede: gerenciar a rede de computadores, incluindo configuração de rotas, endereçamento IP, monitoramento de tráfego, gerenciamento de servidores, entre outros;

Treinamento de usuários: treinar usuários em novas tecnologias e aplicações, orientando-os quanto à utilização adequada de *softwares* e equipamentos;

Documentação: manter a documentação técnica atualizada, incluindo manuais de instrução, procedimentos operacionais e histórico de manutenção.

3.9.4 Equipe Administrativa

Competências: Promover a organização e acompanhamento dos contratos, processos administrativos, adequação quanto às normas e regulamentações aplicáveis ao setor público, incluindo privacidade de dados, segurança cibernética, licitações e contratos públicos; acompanhamento dos processos eletrônicos e trâmites legais; controle e documentação dos ativos de rede; agendas e organização das visitas técnicas; controlar os recursos financeiros de dotação orçamentária do setor; acompanhar os processos de compras e/ou pagamentos aos fornecedores etc.

3.9.5 Equipe de Sistemas

Competências: As principais competências da equipe de sistemas estão no acompanhamento de desenvolvimento de sistemas realizados por terceiros, desenvolvimento personalizado para atender a demandas específicas de determinados setores, gerenciamento de segurança e atualização de *softwares*, gerenciamento de *backup* e recuperação para que possam garantir a segurança e integridade dos sistemas públicos, gerenciamento de projetos de sistemas, incluindo a análise de requisitos, planejamento, execução e controle.

3.10 OBJETIVOS

Os objetivos estratégicos da Divisão de Inovação e Tecnologia, devidamente alinhados aos objetivos estratégicos da gestão municipal, apresentam-se como tangíveis dentro de um prazo de 03 (três) anos, de 2025 a 2027. Porém, a volatilidade do segmento de tecnologia da informação exige manutenção constante do plano, haja vista a possibilidade de mudanças de tendências.

ITEM	OBJETIVO
01	Melhorar as condições de trabalho da equipe da DIT com aplicação de cursos de qualificação profissional.
02	Melhorar a comunicação remota entre as unidades com vistas ao ganho de desempenho.
03	Consolidar a infraestrutura dos demais setores com aquisição de novos equipamentos, upgrades estruturais e readequações.
04	Atualizar a DIT com aquisição de novos equipamentos mais modernos.
05	Promover a segurança lógica da rede e soluções de armazenamento seguro.
06	Aprimorar o processo de atendimento a usuários.
07	Implantar novos sistemas de trabalho para automatizar a rotina, procedimentos e reduzir os custos operacionais.

4. DIAGNÓSTICO DE TECNOLOGIA DA INFORMAÇÃO

4.1 INTRODUÇÃO

Diagnosticar as fraquezas de uma organização é uma tarefa essencial para a melhoria contínua dos ganhos de produtividade. O Diagnóstico de Tecnologia da Informação acaba por legitimar meios para a tomada futura de decisões que mitiguem os riscos e reduzam os custos relacionados aos eventuais incidentes de Tecnologia da Informação (TI).

A elaboração deste plano permitiu que a Prefeitura pudesse avaliar os ativos de Tecnologia da Informação da Prefeitura de Bragança Paulista e sua aderência para a definição das melhores práticas de mercado e de fabricantes, além das normas de tecnologia da informação.

4.2 VISÃO GERAL

O ambiente de tecnologia da informação da gestão municipal da Prefeitura do Município de Bragança Paulista é composto dos seguintes ativos (dados de referência atualizados em 2025)¹:

ATIVO	QUANTIDADE
Servidores de Rede (Físico)	7
Servidores de Rede (Físico) em regime de comodato	2
Switch camada 2 (não gerenciados)	> 200
Switch camada 2 (gerenciados)	≅ 50
Estações de trabalho	≅ 1.500
Multifuncionais PB/Color A4/A3 e LaserJet (apenas impressora)	≅ 430
Nobreaks 2/3kVA	4
Nobreaks 600/800/1200 VA	> 50
Link de Fibra Óptica com SLA > 99% (1 Gbps, 500 Mbps, 400 Mbps) dedicado	10
Usuários AD	≅ 1004
Pontos de Acesso à Cidade Digital (Wi-Fi) Público – Endereços distintos	31
Banda larga mínima por unidade (próprio) público	600 Mbps Down / 300 Mbps Upload
Telefonia com troncos SIP / DDR / E1 Digital	16
Total de Próprios atendidos com telefonia/conexão de Internet	305

¹ Os servidores físicos municipais são compostos ora por sistemas operacionais instalados diretamente no *hardware* e alguns com sistema de virtualização (*Hipervisores*) por *hardware (bare-metal)* com diversas VMs (*Virtual Machines*) em operação.

4.3 INFRAESTRUTURA

As próximas seções deste documento apresentam as disposições físicas e lógicas do ambiente de tecnologia da informação da Prefeitura de Bragança Paulista, assim como a identificação de deficiências e necessidades de adaptações e reformulações consideradas de grau médio e alto para um ambiente tão dependente de tecnologia da informação.

4.3.1 ESTAÇÕES DE TRABALHO E SERVIDORES

Todo o parque tecnológico municipal é equipado com diversos sistemas operacionais, todos com ferramentas básicas para escritório (pacote *office*, leitores de PDF etc.). Os diversos servidores são equipados com os sistemas operacionais Microsoft e Linux, que por questões de segurança têm omitidas as versões dos sistemas operacionais, dos bancos de dados, bem como as versões dos demais sistemas existentes.

Setores específicos como Secretaria Municipal de Obras, Secretaria Municipal de Meio Ambiente, Secretaria Municipal de Planejamento, dentre outras, possuem licenças de uso de *software* do Pacote *AEC Collection* da Autodesk, pelas quais são realizados todos os projetos e acompanhamento com BIM (*Building Information Modelling* – Modelagem da Informação da Construção).

4.3.2 ESTRUTURAS DE REDE DA PREFEITURA DE BRAGANÇA PAULISTA

LOCAL	DEFICIÊNCIA	GRAU DE RISCO	NECESSIDADE DE ADAPTAÇÃO
Datacenter 1 e 2	Infraestrutura física – reestruturação do cabeamento estruturado e ambiente físico.	ALTO	Adequação para uma sala mais segura, com novas instalações elétrica e cabeamento estruturado, melhorar a climatização, revitalizar a parte civil (pinturas de paredes e novos tetos) e controle de acesso.
Setor de TI (Sala dos colaboradores)	Uma nova sala com acomodações adequadas de	MÉDIO	Um novo ambiente totalmente adequado ao

	móveis e infraestrutura elétrica e de dados, com bancadas e novos equipamentos eletrônicos para melhorar a qualidade da prestação dos serviços.		que o setor exige para cumprir suas obrigações.
Paço Municipal	Reforma geral da rede de dados e elétrica.	ALTO	Implantação de uma nova rede de dados e voz com nova infraestrutura elétrica.
Secretaria Municipal de Turismo	Reestruturação da Sala Técnica de TI.	ALTO	Substituição da porta para um melhor controle de acesso, reestruturação geral da sala de TI e novas instalações nas work areas.
CCO (Centro de Controle de Operações)	Novas instalações para rede de dados, voz e elétrica.	ALTO	Implantação de um novo ambiente mais moderno, amplo e revitalizado com apoio de sala técnica, novas work areas, com uso de workstation, sala climatizada, com apoio operacional, munidas de redundância de links dedicados de internet e elétrica (gerador).
Próprios Públicos	Reestruturação da rede de dados (cabeamento) e substituição de equipamentos de rede de camada 3 ou superiores.	MÉDIO	Reestruturação geral da rede de dados e voz com uso de cabeamento estruturado com no mínimo cabos de rede cat. 6, com certificação e documentação da rede. Substituição dos equipamentos de rede por modelos atuais de camada 3 ou superiores.

4.3.3 SISTEMAS PRÓPRIOS E TERCEIRIZADOS UTILIZADOS PELA PREFEITURA DO MUNICÍPIO DE BRAGANÇA PAULISTA

Alguns sistemas utilizados pela Prefeitura do Município de Bragança Paulista são próprios e outros terceirizados através de regular processo de licitação.

São próprios e controlados pela DIT os seguintes sistemas:

Sistema de Controle de Processos e Arquivos

Sistema de Controle de Tráfego Pesado

(SMMU, 2017).

Controle de veículos com restrição de tráfego no município.

<https://ctc.braganca.sp.gov.br>

SIPAT

(SESMT, 2020).

Plataforma para acesso controlado de vídeos de treinamento da CIPA.

<https://sesmt.braganca.sp.gov.br>

CIPA

(SESMT, 2017–2020).

Sistema de votação eletrônica para eleições anuais da CIPA.

<https://cipa2020.braganca.sp.gov.br>

GLPI

(DIT, 2020). Ferramenta de *software*

ITSM (Gerenciamento de Serviços de TI). <https://suporte.braganca.sp.gov.br>

WEBGIS

(DIFI, 2015).

Consulta de informações espaciais georreferenciadas e tabulares de um determinado lugar de forma interativa, análises e produção de material cartográfico.

<https://webgis.braganca.sp.gov.br>

O sistema atual de gestão público municipal é mantido por uma empresa privada terceirizada, cuja razão social é Conam Consultoria em Administração Municipal Ltda., sendo a solução composta dos seguintes módulos:

- Módulo de gestão de execução orçamentária, financeira e contábil;

- Módulo de tributos mobiliários (ISS);
- Módulo de tributos imobiliários (IPTU);
- Módulo de imposto sobre transmissão de bens imóveis (ITBI);
- Módulo de dívida ativa;
- Módulo de arrecadação (tesouraria);
- Módulo de controle de cemitérios;
- Módulo de parcelamento *online*;
- Módulo de nota fiscal eletrônica;
- Módulo de compras, licitações e almoxarifado;
- Módulo de pregão presencial (*web*);
- Módulo de contratos;
- Módulo de patrimônio;
- Módulo de administração de frotas;
- Módulo de recursos humanos e folha de pagamento;
- Módulo de portal do servidor;
- Módulo de portal da transparência;
- Módulo de portal de serviços ao cidadão;
- Módulo de portal do empreendedor;
- Módulo de controle interno;
- Módulo de protocolo e arquivo;
- Módulo de *Business Intelligence* (BI);
- Módulo de *backup* em nuvem.

O sistema público de Ouvidoria Municipal também é mantido por uma empresa privada terceirizada, cuja razão social é Webnets Soluções Eireli, e, por fim, o sistema de gerenciamento de e-mails corporativos com a empresa Endurance Brasil.

A Secretaria de Saúde conta com empresa privada terceirizada para gestão do aplicativo é-Saúde Bragança Paulista, cuja razão social é Troupe Tecnologia.

A Secretaria de Educação está realizando estudos para aquisição de sistema de gestão para a respectiva pasta.

4.3.4 SEGURANÇA

A Prefeitura Municipal de Bragança Paulista possui em seus computadores sistemas operacionais equipados com antivírus homologados e, nos servidores, conta com solução de antivírus em *cloud* com proteção avançada de detecção, visibilidade e resposta em nuvem.

Com solução de *firewall* com funcionalidades de *multi-WAN* com balanceamento de carga e/ou *failover*, promovendo uma melhora na disponibilidade da internet.

O município possui recursos de VPN com criptografia em *IPSec*, promovendo segurança para os acessos externos. Estas VPNs são estendidas aos usuários que necessitam realizar seus trabalhos em regime de *home office*, modalidade consolidada no município e mantida como prática permanente de trabalho remoto.

O município conta com diversos equipamentos de rede em diversas unidades públicas, provendo segurança de *firewall*, redundância de *link* ou balanceamento de carga.

4.3.5 BACKUP

O município possui diversos tipos de dados e sistemas de banco de dados. Os arquivos em geral passam por *backups* automáticos, sendo realizados através de arranjos como, por exemplo, *Full + Incremental* ou *Full + Diferencial*. Para ambos os casos, os servidores são compostos por RAID e os *backups* salvos em *Storage* tipo NAS.

Os *backups* dos sistemas gerenciados por empresas terceirizadas são realizados, no mínimo, diariamente, com criação de *snapshots* para facilitar o restabelecimento do serviço em caso de desastre. Cópias semanais destes *backups* de terceiros são realizadas nos servidores do município.

4.3.6 PESSOAS E PROCESSOS

Os atuais prestadores de serviço da Prefeitura do Município de Bragança Paulista, no segmento de tecnologia da informação, são:

EMPRESA	OBJETO
---------	--------

CONAM Consultoria em Administração Municipal Ltda.	Sistema de Gestão Público municipal.
INFOPROTECT Consultoria em Tecnologia da Informação Ltda.	Solução IaaS para os serviços de e-mail e hospedagem dos sites, com 2 IPs públicos dedicados, DNS, recursos de transferências ilimitadas, 2 TB de disco em RAID, 16 GB de RAM e 4 vCPU Xeon 2,1 GHz, dentre outros recursos.
Webnets Soluções Eireli	Solução SaaS do portal eletrônico do município e do sistema de ouvidoria.
Telefônica Brasil S.A.	Provedora de Telefonia STFC, solução de voz avançada (SIP, E1, DDR, FWT).
MÓBILE Comércio e Serviços em Telecomunicações Ltda. – EPP	Contratação de empresa para fornecimento de equipamentos e acessórios em regime de locação.
Simpres Comércio, Locação e Serviços Ltda.	Outsourcing em laptops e impressoras.
Vigilância Solidária Segurança Eletrônica EIRELI	Serviços de gestão especializada de sistemas informatizados, dispositivos eletrônicos e serviços para a implantação de plataforma de gerenciamento integrado de dados, treinamento técnico e manutenções.
M. A. de Toledo Informática ME	Suporte técnico avançado à estrutura de redes de computadores e segurança da informação.
ISP PREMIUM Telecom S/A	Fornecimento de Banda Larga em diversos prédios públicos e Link Dedicado.

Em relação ao atendimento de suporte reativo, se o problema for lógico em nível de *software*, é realizado o acesso remoto para sua resolução. Em relação ao atendimento de suporte preventivo, há política definida para atualização dos *softwares* e sistemas operacionais das estações de trabalho e servidores.

5. INFRAESTRUTURA FÍSICA E LÓGICA DA REDE DE COMPUTADORES

Projeto de infraestrutura física e lógica para adequações das unidades públicas, garantindo a eficácia dos serviços providos por sistemas automatizados, oferecendo condições ideais de segurança e disponibilidade para acomodação de equipamentos de tecnologia da informação, que compreende a criação, instalação e configuração de uma determinada rede de computadores para atender às necessidades do setor público. Esse projeto leva em consideração diversos fatores, como o tamanho do setor, o número de usuários, a distância geográfica entre os usuários e a disponibilidade de recursos financeiros. Durante o projeto são observados:

Definição de requisitos: identificação das necessidades da organização, incluindo o número de usuários, tipo de dados que serão transmitidos e as aplicações que serão usadas;

Projeto lógico: criação de um diagrama lógico da rede, definindo as principais funcionalidades e padrões a serem utilizados;

Projeto físico: criação de um diagrama físico da rede, definindo os equipamentos necessários, como roteadores, *switches*, cabos e servidores, e a disposição desses equipamentos no espaço físico;

Definição de equipamentos: definição de equipamentos de rede apropriados para o projeto, levando em consideração o tamanho da rede, o orçamento disponível e os recursos necessários;

Instalação de equipamentos: instalação e configuração dos equipamentos de rede, incluindo a conexão física dos dispositivos e a configuração dos endereços IP e outros parâmetros de rede;

Teste de rede: realização de testes de conectividade e desempenho para garantir que a rede esteja em pleno funcionamento;

Implementação de políticas de segurança: implementação de políticas de segurança para proteger a rede contra ameaças cibernéticas e violações de segurança.

6. REDE FÍSICA

A estrutura de comunicação de uma organização é fundamental para a melhoria de processos administrativos e redução de custos operacionais. A Prefeitura do Município de Bragança Paulista necessita de atualização contínua em sua infraestrutura de rede física para assegurar mais estabilidade e escalabilidade na comunicação de dados, além de preparar sua infraestrutura para as novas tecnologias de comunicação emergentes.

Com o crescimento das plataformas de transmissão de dados, crescimento do quadro de agentes públicos e aumento da demanda por serviços eletrônicos, passou-se a exigir um constante aumento, tanto na abrangência quanto na capacidade da rede atual, mostrando assim uma deficiência do sistema existente e expondo a necessidade de uma nova infraestrutura planejada. Este projeto deverá satisfazer, no mínimo, os seguintes objetivos:

- Garantir segurança física dos equipamentos de tecnologia da informação e, conseqüentemente, a proteção física contra acesso indevido;
- Garantir o condicionamento adequado dos equipamentos de tecnologia da informação para o provimento de suas funções;
- Prevenir desastres no ambiente de tecnologia da informação causados por fenômenos naturais ou falhas humanas;
- Reformular toda a estrutura de cabeamento de dados.

7. SEGURANÇA

Vivemos em um mundo globalizado, com o espaço geográfico fragmentado, porém fortemente articulado pelas redes, onde a informação, independente do seu formato, é um dos maiores patrimônios de uma organização moderna, sendo vital para quaisquer níveis hierárquicos e dentro de qualquer instituição que deseja manter-se competitiva.

Considerada um quesito importantíssimo para a realização do negócio, a informação deve ser protegida e gerenciada. Nos últimos anos, as tecnologias de

informação e comunicação têm evoluído de forma rápida, fazendo com que as organizações tenham maior eficiência e rapidez nas tomadas de decisão; devido a este fato, as chances de uma organização não usar sistemas de informação tornaram-se praticamente nulas.

Neste contexto, a importância de se utilizar mecanismos de segurança é vital para a continuidade dos serviços. O município, por meio da equipe da DIT, realiza:

Políticas de segurança: garantia de que as políticas de segurança da informação estejam atualizadas e que todos os funcionários tenham conhecimento e adotem as medidas de segurança necessárias;

Controles de acesso: garantia de que os controles de acesso estejam implementados corretamente, permitindo que apenas pessoas autorizadas acessem informações sensíveis;

Proteção de dados: garantia de que os dados sensíveis estejam protegidos contra perda, roubo ou acesso não autorizado, em conformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei Federal n.º 13.709/2018);

Treinamento: garantia de que todos os funcionários tenham treinamento suficiente em segurança da informação, para que estejam cientes dos riscos e saibam como proteger as informações do município;

Monitoramento e detecção de ameaças: monitoramento da rede e dos sistemas da prefeitura em busca de possíveis ameaças, implementando medidas para detectar e responder rapidamente a qualquer incidente de segurança;

Atualizações de software: garantia de que todos os *softwares* utilizados na prefeitura estejam atualizados e protegidos contra vulnerabilidades conhecidas;

Backup: garantia de que os dados da prefeitura estejam sendo regularmente salvos e armazenados em local seguro, para que possam ser recuperados em caso de perda ou danos.

8. FIREWALL DE PERÍMETRO

Quando a rede corporativa é conectada à Internet, garantir a segurança contra intrusos passa a ser de grande importância. Há diversos conceitos e mecanismos de proteção entre a rede local e a Internet. Os mecanismos de segurança de borda são utilizados para proteger as redes de computadores contra ameaças externas, tais como ataques cibernéticos, *malware*, *phishing*, entre outros. Destacam-se os principais mecanismos:

Proteção da rede: proteger contra ameaças externas, evitando que *hackers* e outros criminosos virtuais acessem informações sensíveis ou causem danos ao sistema;

Controle do tráfego de rede: os mecanismos de segurança de borda permitem que o tráfego de rede seja controlado, limitando o acesso de usuários e dispositivos a determinados recursos e informações da rede, garantindo que apenas usuários autorizados tenham acesso aos recursos necessários para realizar suas tarefas;

Deteção e prevenção de ataques: os mecanismos de segurança de borda incluem recursos para detectar e prevenir ataques, como *firewalls*, sistemas de detecção de intrusão (IDS) e sistemas de prevenção de intrusão (IPS), entre outros;

Garantia da conformidade com as políticas de segurança: os mecanismos de segurança de borda permitem que as políticas de segurança do município sejam implementadas e monitoradas de forma mais eficiente, garantindo conformidade com as leis, regulamentações e políticas de segurança vigentes;

Proteção da reputação municipal: a utilização de mecanismos de segurança de borda pode ajudar a proteger a reputação do município, evitando que seja vítima de ataques cibernéticos e outros incidentes de segurança que possam prejudicar sua imagem perante os munícipes e o público em geral.

9. TRABALHO REMOTO

No atual ambiente, em que funcionários estão sempre em movimento, a capacidade de acessar informações essenciais a partir de qualquer lugar não é um luxo, mas uma necessidade.

O acesso remoto pode permitir que pessoas não autorizadas tenham acesso a dados sensíveis ou confidenciais do município e, para tanto, destacam-se os seguintes itens para garantia da segurança no acesso remoto aos servidores/dados do município:

Autenticação forte: utilização de sistema de autenticação forte, como senhas fortes, autenticação de dois fatores ou autenticação biométrica, garantindo que apenas usuários autorizados tenham acesso remoto aos recursos do município;

Utilização de VPN (Rede Privada Virtual): a VPN estabelece uma conexão criptografada e segura entre o dispositivo do usuário remoto e a rede local do município, permitindo que o funcionário acesse os recursos como se estivesse fisicamente presente na rede interna;

Utilização de Firewall: o *firewall* ajuda a controlar o acesso remoto à rede e protegê-la contra ataques cibernéticos;

Verificação de segurança de dispositivos: exigir que os usuários remotos verifiquem a segurança de seus dispositivos antes de acessar os recursos da organização, incluindo a instalação de *software* antivírus, a aplicação de *patches* de segurança e a verificação de vulnerabilidades;

Monitoramento e registro de atividades: realizar o monitoramento e registro das atividades de acesso remoto para identificar possíveis ameaças de segurança e garantir que os funcionários estejam cumprindo as políticas de segurança estabelecidas;

Treinamento: realização de treinamentos e programas de conscientização de segurança para educar os funcionários remotos sobre as melhores práticas de segurança e os riscos associados ao acesso remoto.

10. CONTROLE DE ACESSO À REDE

O acesso à rede de dados do município é disponível a qualquer funcionário e este acesso poderá ocorrer de forma local ou remota. Para garantir a segurança, o controle de acesso e o monitoramento, deve ser aplicado:

Política de senhas fortes: ajuda a garantir que apenas usuários autorizados tenham acesso à rede, com exigência de senhas longas e complexas, além de exigir que os funcionários as troquem regularmente;

Restrições de acesso: restringir o acesso a recursos de rede apenas para usuários autorizados e definir permissões de acesso de acordo com o papel (ACL) e a responsabilidade de cada usuário;

Criptografia: utilizar a criptografia para proteger os dados que trafegam na rede, utilizando protocolos como o TLS (*Transport Layer Security*) ou SSL (*Secure Sockets Layer*);

Firewall: utilizar *firewalls* para controlar o acesso à rede e protegê-la contra ameaças externas, bloqueando os acessos não autorizados;

Monitoramento de atividades: monitorar as atividades de rede para identificar possíveis ameaças de segurança e tomar medidas preventivas ou corretivas;

Atualizações de segurança: manter os sistemas operacionais (servidores e estações) atualizados com as últimas atualizações de segurança e *patches* de correção de vulnerabilidades;

Treinamento dos colaboradores: oferecer treinamentos e conscientização de segurança para os usuários da rede, destacando a importância de manter senhas fortes, não compartilhar credenciais de acesso e estar atento a possíveis ameaças;

Controle de acesso físico: controlar o acesso físico aos servidores e equipamentos de rede, mantendo-os em local seguro e com acesso restrito apenas para pessoas autorizadas.

11. INVENTÁRIO

O inventário é fundamental para o gerenciamento eficiente e seguro de uma rede de computadores, permitindo a gestão sobre os ativos de TI do município, auxiliando nas tomadas de decisões do setor de tecnologia quanto às atualizações, manutenções e segurança de rede.

O inventário proporciona uma visão macro sobre quais dispositivos estão conectados à rede, suas características e configurações, e quais *softwares* estão sendo executados nesses dispositivos. As principais vantagens de realizar um inventário de rede são:

Identificação de ativos: com o inventário é possível identificar todos os dispositivos conectados à rede, o que inclui servidores, computadores, roteadores, *switches*, impressoras, entre outros;

Gerenciamento de licenças de software: o inventário de rede também ajuda no gerenciamento das licenças de *softwares*, garantindo a conformidade com as licenças adquiridas e ajudando a evitar possíveis multas por uso indevido;

Detecção de problemas de segurança: ajuda a identificar possíveis falhas de segurança na rede, como dispositivos ou *softwares* não atualizados, possibilitando a adoção de medidas para corrigir essas falhas e garantir a segurança da rede;

Planejamento de atualizações e manutenção: é possível saber quais dispositivos e *softwares* precisam de atualizações ou manutenção, podendo ser realizadas essas atividades com antecedência e evitando possíveis interrupções na operação da rede.

12. MONITORAMENTO DA REDE DE DADOS

O monitoramento é importante para o acompanhamento do desempenho da rede, identificação de falhas e problemas de segurança. Por meio do monitoramento da rede, medidas preventivas garantem o funcionamento adequado do sistema. As principais razões pelas quais o monitoramento de rede é importante:

Identificar falhas de hardware: auxilia na identificação de falhas de *hardware* em servidores, roteadores e outros dispositivos de rede antes que causem problemas mais graves, proporcionando uma análise preditiva dos ativos monitorados;

Identificar problemas de desempenho: ajuda na identificação de gargalos de rede e outras questões que afetam o desempenho do sistema, auxiliando na tomada de medidas para otimização da rede;

Monitorar o tráfego de rede: o monitoramento ajuda na identificação de padrões de tráfego incomuns e potenciais ameaças de segurança, como ataques de *malware* ou invasões;

Prever a capacidade de rede: auxilia na previsibilidade da capacidade de rede necessária para suportar o crescimento futuro, garantindo que a infraestrutura de rede seja dimensionada corretamente;

Identificar problemas de conformidade: ajuda a identificar potenciais violações de conformidade com políticas internas, leis e regulamentações, auxiliando na adoção de medidas corretivas apropriadas.

13. POLÍTICA DE SEGURANÇA

A Política de Segurança é fundamental para garantir a proteção adequada das informações sensíveis e críticas do município, minimizando o risco de violações e garantindo que os usuários sigam as melhores práticas de segurança da informação.

A política deve incluir diretrizes e procedimentos claros para proteger a infraestrutura de TI e os dados armazenados, além de estabelecer padrões de comportamento seguro para os usuários. As principais diretrizes e procedimentos que devem ser incluídos em uma política de segurança para o setor de TI são:

Autenticação e controle de acesso: definição de políticas claras para autenticação e controle de acesso a sistemas e aplicativos, incluindo a utilização de senhas fortes, controle de acesso baseado em função e gerenciamento de credenciais de usuários;

Monitoramento e gerenciamento de ameaças: a política deve estabelecer procedimentos para o monitoramento de ameaças à rede e aos sistemas, além de definir planos de contingência e recuperação em caso de violação de segurança;

Atualização e manutenção de software: é importante estabelecer procedimentos para a atualização e manutenção de *softwares*, incluindo a instalação de *patches* de segurança e atualizações de sistemas operacionais;

Gerenciamento de dispositivos móveis: a política deve incluir diretrizes claras para o gerenciamento de dispositivos móveis, como *smartphones* e *tablets*, que acessam a rede municipal;

Treinamento dos colaboradores: é fundamental que a política abranja o treinamento e a conscientização dos usuários sobre a importância da segurança da informação e as melhores práticas para manter a rede segura.

14. PLANO DE CONTINUIDADE DE NEGÓCIO

A elaboração deste plano envolve todas as atividades necessárias para garantir que todos os processos de negócios críticos da Prefeitura Municipal de Bragança Paulista sejam contemplados numa solução de continuidade, que busca o menor custo operacional possível.

O plano de continuidade permite a recuperação de sistemas e serviços de TI, garantindo a continuidade das operações críticas em caso de desastres naturais, falhas de sistemas ou outras interrupções não planejadas. Dentre as principais etapas envolvidas no plano de continuidade de negócio, destaca-se:

Identificação de recursos críticos: identificação dos sistemas, aplicativos e dados críticos que precisam ser restaurados com prioridade após uma interrupção;

Avaliação de riscos: avaliação dos riscos que podem afetar a continuidade dos serviços de TI e definição de medidas de prevenção e contingência;

Desenvolvimento de estratégias de recuperação: definição de estratégias para recuperação de dados, sistemas e serviços críticos, incluindo *backup* e recuperação de desastres;

Testes e validação: realização de testes regulares, com periodicidade mínima anual, para validar a eficácia do plano de continuidade de negócio e identificar eventuais lacunas ou problemas a serem resolvidos;

Manutenção e atualização do plano: o plano de continuidade de negócio de TI deve ser mantido atualizado e revisado regularmente para garantir que reflita as necessidades e mudanças do setor público.

15. CONSIDERAÇÕES FINAIS

A falta de investimentos em *hardwares*, *softwares*, equipamentos, sistemas operacionais, gerenciadores de banco de dados, além da ausência de procedimentos formais, conduz a um ambiente desprovido de padrões e suscetível a vulnerabilidades. Não há sistemas e equipamentos redundantes para provimento de serviços de missão crítica em escala ideal, além de uma equipe técnica enxuta e responsável por uma grande quantidade de atividades associadas à unidade de tecnologia da informação.

Por outro lado, observa-se que, a despeito das deficiências acima descritas e das limitações orçamentárias, há uma preocupação contínua na reversão do quadro atual, reforçada pela atualização deste PDTIC para o triênio 2025–2027.

O setor de TI tem um papel crucial na gestão da informação e no suporte às atividades da administração. A implementação de políticas e processos de segurança da informação, o desenvolvimento de planos de continuidade de negócio e a adoção de tecnologias de ponta são algumas das estratégias que podem ser adotadas para garantir a eficácia do setor de TI no município.

É importante destacar que, em um ambiente de TI, a constante atualização e o aprimoramento das habilidades técnicas são fundamentais para manter-se alinhado às novas tendências e tecnologias emergentes. Além disso, a colaboração e o trabalho em equipe são essenciais para garantir a qualidade e a eficácia dos serviços prestados.

Em resumo, o setor de TI da Prefeitura Municipal de Bragança Paulista deve ser gerenciado com excelência e profissionalismo, visando garantir a segurança, a confiabilidade e a disponibilidade dos sistemas e informações, bem como a eficácia da administração pública em geral.

Após a leitura e análise deste documento, consideramos o mesmo **HOMOLOGADO** e apto para orientar nossas metas quanto ao uso de nossos recursos de tecnologia e informação de nossa instituição no triênio 2025–2027.

Bragança Paulista/SP, 17 de junho de 2025.

Edmir José Abi Chedid

Prefeito Municipal

André Elesbão

Secretária Municipal de Governo, Desenvolvimento Econômico e Inovação

Everton Ferreira

Chefe da Divisão de Inovação e Tecnologia